FSA Security Incident Implementation Guide

May 2003

Table of Contents

Draft
FSA Implementation Guide

1.0 INTRODUCTION

This document is based upon the security incident response guidelines from the Department of Education's Education Computer Incident Response Center (EDCIRC). *The EDCIRC documents on incident response are the primary sources that must be consulted and followed.* FSA maintains a unique dependence upon variety of contractors to operate their systems which is not found elsewhere in the Department of Education. This document is written to directly address FSA's roles, responsibilities and expectations for incident response.

Appendix B and C of the Department's Incident Handling Guide specifically addresses the reporting guidelines for both Security Incidents and Suspicious Activity. Since EDCIRC will be providing investigative, forensics and analysis capabilities for most, if not all systems, reporting incidents and suspicious activity will most directly affect FSA and their contractors.

1.1 Purpose

All Federal agencies are required by law to have within their Information Technology security programs an incident handling and reporting capability. FSA and its contracted partners operate a large number of systems at numerous locations using many different software platforms. While these systems are constructed securely, incidents will inevitably occur. The direct purpose of this document is to provide guidance to FSA staff and contractors for implementing the procedures on security incident and suspicious activity handling and reporting as written in the Department's Incident Handling Guide.

1.2 Scope

FSA's Implementation Guide is designed to help personnel at FSA understand their roles and responsibilities in the incident response process. It includes plans for notifying affected parties, escalating responses through the chain-of-command, and coordinating with the Departmental incident response team (if necessary). It is important that security personnel (SSO's, etc.) and those who work directly with computer systems understand and follow this document.

1.3 Document Structure

The document is divided into four sections and an appendix. Section 1.0 is an introduction and to provides important definitions. Section 2.0 discusses monitoring and review of system and network logs. Section 3.0 describes the specifics for FSA on Security Incident Reporting. This comprises a discussion on communicating security incidents, the detailed responsibilities of each of the affected parties, and how they interact with each other. Section 4.0 focuses on the reporting of Suspicious Activity including the necessary steps and reports and time frames required.

1.4 Definitions

An effective Incident Response Program requires that certain terms be defined in a precise way to avoid confusion. FSA utilizes the Department's definitions as the baseline and also provides clarification by providing industry-recognized definitions; predominately based on the National Security Agency (NSA) National Security Telecommunications and Information Systems Security Committee (NSTISSI) 4009 document.

These definitions give basic qualifying information for identifying security incidents and suspicious activity. This information must be combined with common sense, discretion and diligent professional interpretation of any activity in order to adequately identify incidents or suspicious activity.

Computer Security Incident and Suspicious Activity Definitions

Computer Security Incident (EDCIRC)	*Any event that has resulted in: unauthorized access to, or disclosure of, sensitive information; unauthorized modification or destruction of system data; reduced, interrupted, or terminated data processing capability; introduction of malicious program or virus activity; or the degradation or loss of the systems Confidentiality, Integrity or Availability; or the loss, theft, damage, or destruction of an IT resource.* Examples of computer security incidents include: unauthorized network scans or probes; successful and unsuccessful system intrusions; unauthorized use of system privileges; and, execution of malicious code on an IT resource. (See Schedule A -- Incident Reporting & Response Guidance: Types of Incidents Matrix for more examples.)
Suspicious Activity (EDCIRC)	*Any activity that is considered: an abnormal system event occurrence for a given system that cannot be immediately explained, but does not pose an immediate threat; observed recurring activity that possibly indicates attempts are being made to exploit a vulnerability but is countered by security controls in place; sporadic repeated activity that cannot be readily explained by system operations and security staff; activity that, when combined with other factors or anomalous events,* ***indicates a possible cause for concern****.* Examples of suspicious activity include: unusual usage patterns, misuse of computer system resources, or multiple attempts to log into a user account that have proven unsuccessful. (See Schedule B -- Incident Reporting & Response Guidance: Types of Incidents Matrix for more examples.)

The definitions, as provided above, should be sufficient to identify Security Incidents and Suspicious Activity. With the objective of providing more precise definitions for security incidents and to show how it ties into overall Information Assurance FSA provide the table below.

NSTISSI 4009 Computer Security Incident Definitions

Term		Definition
Information Assurance (NSTISSI 4009)		Information operations that protect and defend information and information systems by ensuring their availability, integrity, authentication, confidentiality, and non-repudiation.
IA INCIDENT TYPES	**Attack**	Involving the intentional act of attempting to bypass one or more Information Assurance Security Controls of an Information System (IS).
	Compromise	Where information is disclosed to unauthorized persons or a violation of the security policy of a system in which unauthorized internal or unintentional disclosure, modification, destruction, or loss of an object may have occurred.
	Contamination	Involving the introduction of data of one security classification or security category into data of a lower security classification or different security category.
	Denial of Service (NSTISSI 4009)	Type of incident resulting from any action or series of actions that prevents any part of an IS from functioning.
Compromised System (Based on NSTISSI 4009)		Is a system for which security measures fail to provide Information Assurance (IA).
Security Incident (Based on NSTISSI 4009)		Is an assessed occurrence resulting in a compromised system. This means that at least one the IA incident types was not stopped by currently implemented security measures.
Only when security policies and implementations fail to protect a system from these industry-recognized standards, has a security incident occurred.		

One of the primary goals in FSA is Information Assurance – maintaining information systems integrity, availability, authentication, confidentiality and non-repudiation. Incident Response is an important facet within information assurance because it addresses the actions that need to occur in and when a compromise to information occurs.

2.0 MONITORING SYSTEMS, KEEPING AND REVIEWING LOGS

Audit logs are critical to incident response activities, for a variety of reasons. Periodic review of audit logs helps technical personnel establish a baseline of system activity. Once the personnel have an idea of the baseline, it makes it easier to recognize anomalies in subsequent log reviews. Early identification of anomalies consequently makes it easier to proactively defend the system from attackers.

The following items are the minimum requirements for all systems in regards to monitoring, logging, log review and log retention:

- Maintain sufficient monitoring/logging capability (see Department guidelines)
- Establish typical activity levels or thresholds for system events on each system.
- Monitor and log all systems and system activities (see Department guidelines).
- Someone familiar with the system must review all systems logs and audits at least once a day for any events or series of events that could indicate a breach in security.
- Document the review.
- Each system must retain a copy of all audit logs. Section 4.3 of the FSA Security Policy states that such logs will be kept for a minimum of one year.
- Remain alert for behaviour that is obviously out of place or wrong (e.g. web defacements and Denial of Service attacks etc.).

To avoid confusion, FSA refers to the routine inspection of logs and audits for Suspicious Activity or Security Incidents as a "log review". Log reviews can be accomplished through automated and/or manual methods and tools. The terms "analysis" and "log analysis" are terms that refer to a scrutinized inspection of data, logs and audits after Activity or Incidents are identified.

2.1 Security Incident VS. Suspicious Activity

"What are we looking for?" is the first question that is commonly asked when thinking about Incident Response. The Department's Incident Reporting Guide only provides common examples. However, each system will have different activity and toleration levels for certain types of activity which only familiarity with the system will indicate. Therefore, only a general description and some possible examples of what to look for can be given. The objective of incident response is to detect a Security Incident or Suspicious Activity as defined and discussed in section 1.4 of this document.

Typically, there is activity on the logs that does not follow the general rules of the system but does not necessarily make it "suspicious activity" or a "security incident". Such an assessment would be made when logs are compared to a base-lined activity log. If the noted activity is different or crosses specified thresholds, or is of a distinctly different nature, then there is probably good cause for concern and gives reason to call the event "suspicious activity". Actually identifying an issue of concern as a "security incident" entails being able to positively know and/or show that a compromise has occurred. Moving an issue previously considered a "suspicious activity" into the category of a "security incident" requires research and analysis.

3.0 REPORTING SECURITY INCIDENTS

The following table provides a concise view of what actions stakeholders should take in response to security incidents. The activities are presented chronologically starting with row one (1). Note rows 8, and 11 actions start in the EDCIRC column.

3.0 Table – Security Incident Handling Process

Contractors	FSA	Ed or EDCIRC	
1) Monitor and Review systems and logs			
2) Security Incident identified			
3) Immediately notify FSA for authority to take system off-line	**3a)** Approve System to go off-line and notify EDCIRC of decision		
4) If instructed, take system off-line, isolate and freeze.			
5) Complete incident form and follow reporting chain. (See Diagram 3.2)	**5a)** SSO reviews Report relays it to CSO, CSO to EDCIRC	**5b)** EDCIRC reviews report – Provides feedback and "next-step" information. Notifies FEDCIRC and others as necessary.	
6) Follow instruction from EDCIRC	**6a)** Follow instruction from EDCIRC		
7) Provide status on actions taken	**7a)** Receive contractor status	**7b)** Receive contractor status	
		STATUS REPORTS	**8)** Analysis of Incident data and system, forensics/ investigate
9) Propose alternate/backup system Wait for approval	**9a)** Receive alt. request- Approve		
10) Implement alt. system			
11b) Receive Findings Report Consult on course of action.	**11a)** Receive Findings Report Consult on course of action		**11)** Analysis complete and findings submitted. Course of action proposed.
12) Course of action followed and completed.			
13) Security Incident resolved Request system reestablishment Wait for approval.	**13a)** System re-establishment approved.		
14) Lessons Learned			

Once an Incident is identified the following chain of action will be set into motion. (Refer to the FSA Incident Response Contact List for contact information. See also 3.2 Diagram – Security Incident Reporting , and 3.3 Table – Security Incident Timelines summary). Please note that while contractors, FSA and the Department must all work together for resolution, each group does have specific responsibilities.

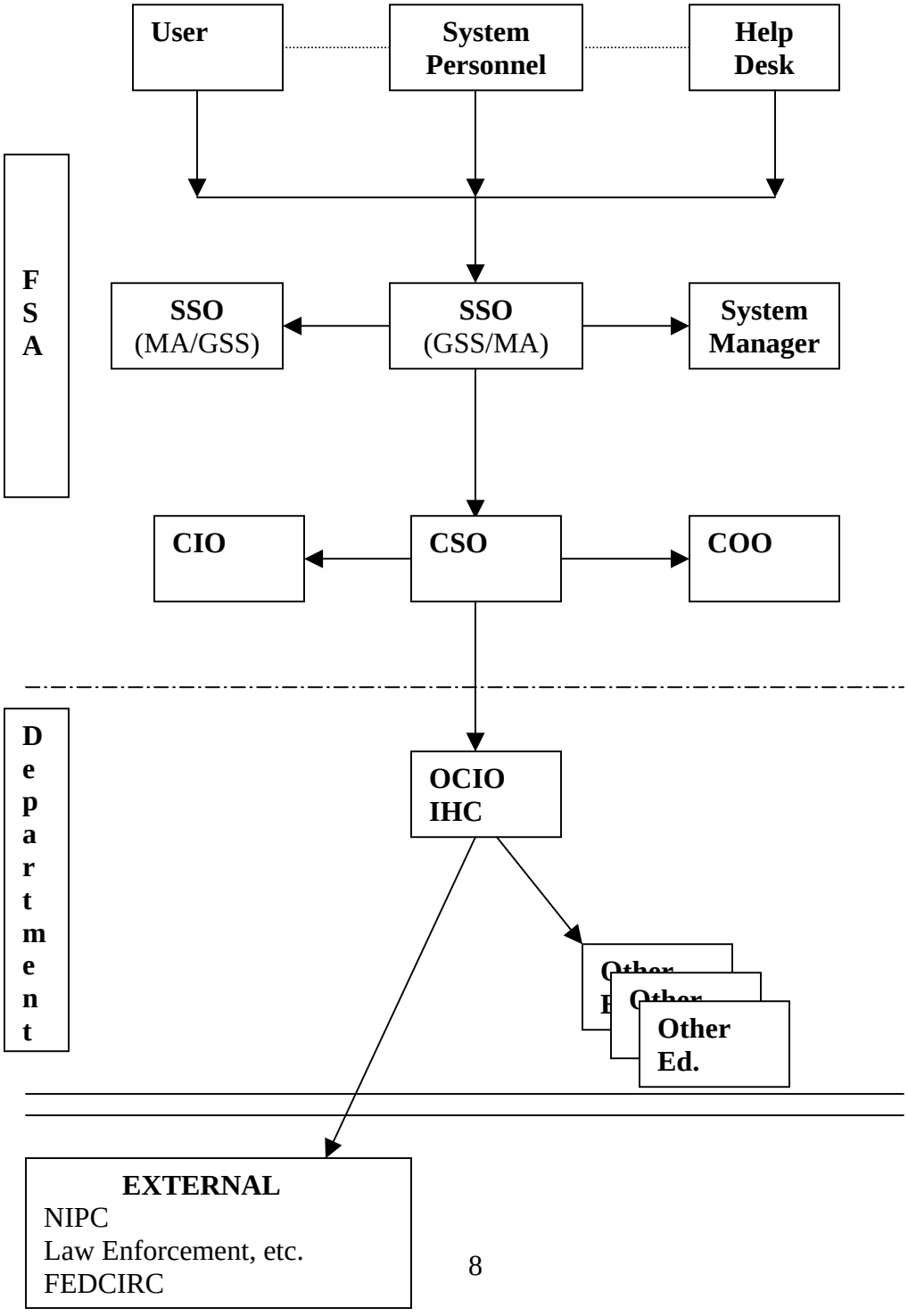
3.1 FSA Security Incident Reporting Action Chain

- Any observed activity that may indicate a computer security incident has occurred must be reported immediately to the relevant System Security Officer (SSO) or security administrator by telephone, email or fax. The reporting party must receive "confirmation of receipt" from the relevant SSO or security administrator; and, it is the responsibility of the reporting party to note the time receipt was confirmed. *If the relevant SSO or Security Administrator is not available by telephone, email or fax, the reporting party must notify FSA's CSO using the same process and receipt confirmation.* (See attached Suspicious Activity Report (SER) form for identification of the information that should be reported.) SSOs, Computer Security Officers (CSOs) and other FSA staff will be trained concerning observable indicators that suggest an incident may have occurred.
- The SSO will ensure that all information on the Suspicious Activity Report (SER) has been filled out. The SSO must then notify FSA's CSO or Deputy CSO by telephone, email or fax within **one (1) hour** of receiving the initial SER. *If the CSO has not confirmed receipt within one (1) hour of notification, the reporting party must notify the Deputy CIO using the same process and receipt confirmation.*
- If it is a General Support System (GSS) that reports the Security Incident, then the SSO for that GSS will notify the SSO(s) of any and all Major Application systems directly affected by that particular GSS and keep them informed for the duration of the Incident. If it is a Major Application system (MA) that reports the Security Incident, then the SSO for that MA will notify the SSO(s) of the GSS the Major Application works with and keep them informed for the duration of the Incident.
- The reporting SSO will also notify the appropriate System Manager
- The CSO reviews the initial SER, and related information to determine whether a potential incident has occurred. The CSO then reports the potential incident and all related information to the Office of the Chief Information Officer (OCIO) Incident Handling Coordinator within **three (3) hours** of receiving the initial report. All information will be included in a report to the OCIO Incident Handling Coordinator.
- The CSO will at the same time notify and send a report to both the CIO and COO.
- The OCIO Incident Handling Coordinator will make a determination for next steps using Department incident handling program procedures **within one (1) hour of receiving a SER**. If warranted, the Incident Handling Coordinator may escalate the details of the report to the Deputy CIO. If the security event or suspicious activity is deemed a serious threat to any Department's IT resources or data, the OCIO Incident

Handling Coordinator will activate the Education Computer Incident Response Capability (EDCIRC) procedures and escalate the information to the Deputy CIO.

- The Deputy CIO will review the SER **within one (1) hour** of receipt and determine whether escalation to the CIO is warranted.
- The CIO or the CIO's designee will review the SER within **one (1) hour** of receipt and determine whether escalation to the Deputy Secretary, the Office of the Inspector General, and appropriate external officials is warranted.

3.2 Diagram - FSA Security Incident Reporting Chain



3.3 Table – Security Incident Reporting Chain, Timeline Summary

Position	(Reports Incident using SER form To) Position	Response Time
System Administrator	System Security Officer (SSO)	Immediately
System Security Officer (SSO)	FSA Incident Coordinator or CSO	1 hour
Computer Security Officer (CSO)	Dept. OCIO Incident Handling Coordinator and PO Senior Officers	3 hours
Dept. OCIO Incident Handling Coordinator	Deputy Chief Information Officer	1 hour
Deputy Chief Information Officer	Chief Information Officer	1 hour
Chief Information Officer or CIO's Designee	Deputy Secretary, Inspector General, and others as appropriate	1 hour

3.4 Post-Reporting Actions and Expectations

Once an actual incident is recognized and reported it is imperative that all affected parties continue to support, cooperate and communicate with each other. EDCIRC (or whoever is providing analysis services) will collect data and research the extent of the problem to determine if there are additional suspicious activities or security incidents. This is accomplished primarily through in-depth log and audit analysis. The Contractor must assist and support EDCIRC in this process by immediately providing all details and information as needed or requested.

3.5 Preservation of Evidence

FSA feels it important to reemphasize the Department's position on proper handling of a computer when an incident is identified. Once a system has been taken off-line with the concurrence of a government authority and the coordination of the Incident Handling Coordinator, that system will not be tampered with in any way or brought back on line without authorization from both FSA's and the Department's Incident Handling Coordinators. This action is necessary to ensure preservation of potential criminal evidence and system condition at the time an incident was discovered.

3.6 Alternate Connectivity

At the same time the analysis for a Security Incident is taking place, FSA expects contractors to provide an alternate, secure system that clients may continue to access if there is extended investigation. This alternate system will only be activated upon agreement between FSA Incident Handling Coordinators. This is consistent with FSA's Continuity of Support Plan (COS) and the Disaster Recovery Plan (DR). Some systems with low availability ratings may not have a COS or DR that calls for alternate system processing. In such a case the contractor should make that information known and consult with FSA on how to proceed. The alternate processing proposal should be submitted as soon as possible. FSA and Departmental authority must approve the proposal for the alternate system before it is placed on-line.

3.7 Three-way Consulting

As part of resolving the Security Incident and after receiving the Findings information from a completed investigation/analysis, the Contractor must consult with FSA and the Department and propose a course of action to remedy the problem and prevent its reoccurrence. FSA, Department and Contractor parties must agree upon the course of action before implementation.

3.8 Final Status

Once the Security Incident is resolved, and the agreed upon course of action is completed the Contractor will request approval to reestablish the system or to show final disposition if it is not reestablished. The Contractor must wait until consent is given by Incident Response Coordinators before reestablishing or otherwise disposing of any system involved in a Security Incident.

4.0 REPORTING SUSPICIOUS ACTIVITY

The following table provides a concise view of actions associated with reporting suspicious activity for the major stakeholders. Follow the numbers from lowest to highest to find the next expected action. Please note that on rows 5 and 6 actions start in the EDCIRC column.

4.0 Table - Suspicious Activity Handling Process

Contractors	FSA	Ed or EDCIRC
1) Monitor and Review systems and logs		
2) Suspicious Activity identified		
3) System left on-line		
4) -In Month Report - Category A activities -In Week Report - Category B activities	**4a)** SSO reviews Report relays it to CSO, CSO to EDCIRC	**4b)** EDCIRC reviews Report
		5) Analysis of Activity 1) Allowed activity 2) Inconclusive – mark and monitor 3) Security Incident (see Chart 4)
6b) Take action as advised by EDCIRC.	**6a)** Receive action and feedback report from EDCIRC	**6)** Provides analysis feed back and required action to FSA and Contractor

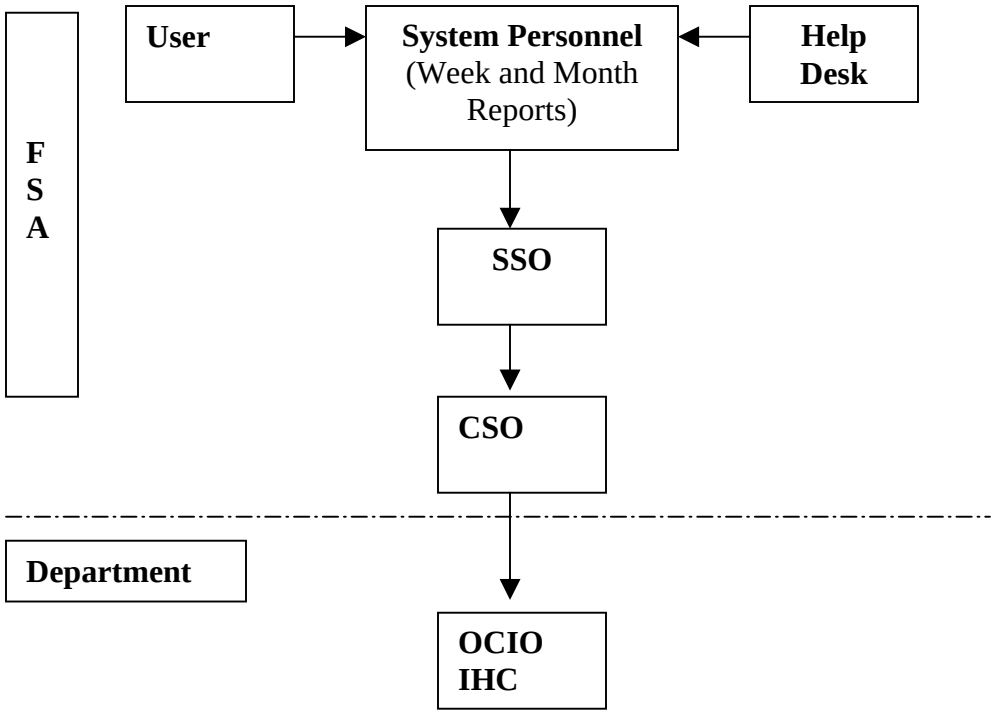
It should be noted that reporting on suspicious activity is quite different from reporting on security incidents. Suspicious activity requires both within the week and within the month reports be submitted. (See also Department's Incident Reporting Guidance, Schedule A and B).

4.1 'Suspicious or Anomalous Activity' Action Chain

The Suspicious Activity Action Chain provided below is written using the Incident Response capabilities provided by EDCIRC. If a FSA Contractor is not using EDCIRC services the requirements of reporting still remain the same. This also means that the Contractor will report on their analysis, findings, and recommendations to the SSO (who will forward the information to the CSO and so on) within the specified timeframe and to show that items are being resolved.

- If, during system log reviews, suspicious activity is discovered, the reviewer will report it to the Security Engineer and thus through the internal contractor channels and also to the SSO who will categorize the activity according to Schedule B -- Incident Reporting & Response Guidance: the Suspicious Activity.
- Category "A" type suspicious activity (which is effectively countered by security controls in place) will be logged and tracked by the system SSO. The SSO will provide a report on this type of activity within a month. Please note that a report can be submitted at any time if there is special concern over a given activity.
- Category "B" type suspicious activity (which is effectively countered by security controls in place but its continued repetition causes additional concern). The SSO will provide a report on this type of activity within a week. Please note that a report can be submitted at any time if there is special concern over a given activity.
- The CSO will review and then forward all Suspicious Activity reports to the Department's Incident Handling Coordinator. The Department's Incident Handling Coordinator will review the reports and within **24-48 hours** of receipt they will convey back any findings and recommended action to the submitting office.

4.2 Diagram - FSA Suspicious Activity Reporting Chain



4.3 Table – Suspicious Activity Reporting Chain, Timeline Summary

Position	(Reports Incident using SER form To) Position	Category A Response Time	Category B Response Time
System Administrator	System Security Officer (SSO)	Within a Month	Within a Week
System Security Officer (SSO)	Computer Security Officer (CSO)	Within a Month	Within a Week
Computer Security Officer (CSO)	OCIO Incident Handling Coordinator	Within a Month	Within a Week
OCIO Incident Handling Coordinator	Back to originating office	24 to 48 hours	24 to 48 hours

4.4 Post-Reporting Actions and Expectations

Once suspicious activity is recognized and reported it is imperative that all affected parties continue to support, cooperate and communicate with each other. The contractor may be asked to compile more data to assist researchers in establishing the extent of the problem and to determine if there are additional suspicious activities or security incidents. The Contractor must be ready to cooperate with EDCIRC in this process and immediately provide all details and information as needed or requested.

In the case of a Suspicious Activity, further analysis will show one of three conclusions: a Security Incident, no cause for concern, or unknown and/or inconclusive requiring monitoring. If the suspicious activity is concluded to be a Security Incident, then the process and procedures for a Security Incident found in this document will be followed. The actions to take for the two remaining conclusions are self-defining.

5.0 Providing All Incident Response Services

Providing all Incident Response Services means incorporating the analysis, forensics and remediation of any security incident or suspicious activity in addition to the monitoring, reviewing, identifying and reporting tasks. Such a program must use the same process that the Department of Education has written throughout their document. Anything more or less must be approved in advance by EDCIRC.

At this time FSA provides only a basic portion of the Incident Response services and relies upon the Department program for analysis, forensics and remediation support.

For informational purposes, the following list is provided to show a high level outline of tasks that are necessary in providing “in-house” total Incident Response capabilities.

- Monitoring
- Reviewing logs and audits
- Identifying
- Reporting
    - Security Incidents
    - Suspicious Activity
        - Weekly Report
        - Monthly Report
- Analysis of reports, logs, audits and data
- Forensics (including legal evidence handling procedures)
- Remediation plan

APPENDIX A - FSA SECURITY INCIDENT CONTACT LIST

Important Notice:

The following FSA Security Incident Contact List is to be used only for FSA Security Incident Response purposes. It is not to be made public or shared with those not involved outside of the Incident Response program.